

I. Section 11(g): Cross-production of a defendant's confidential material to all other defendants

The first dispute pertains to Section 11(g) which governs whether Plaintiff American Patents may cross-produce a defendant's confidential material to another defendant, *e.g.*, in a single expert report or in a motion. ECF No. 160 at 1; ECF No. 161 at 1. After reviewing the Parties' briefing, the Court finds that Defendants' proposed Section 11(g) should be included in the final protective order. But the Court will revisit this issue at the final pretrial conference (or earlier as needed) in order to determine what information needs to be cross-produced. The Court finds that this approach best serves to minimize disclosure of confidential information to potential competitors while also allowing the Parties to properly prepare for trial.

II. Section 8(a): Exceptions to source code designations

The second dispute stems from American Patents' proposal to add the following provision to Section 8(a):

A Producing Party may not designate Discovery Material as HIGHLY CONFIDENTIAL – SOURCE CODE if that Discovery Material is or has been: 1) emailed or otherwise made accessible via a public network or stored on cloud-based servers or on shared drives, or 2) provided to third party developers or similar third parties.

ECF No. 159, Ex. C at 14.

After reviewing the Parties' briefing, the Court finds that American Patents' proposed addition to Section 8(a) should not be included for at least the following reasons. First, the Court agrees with Defendants' contention that just because Defendants' source code is "stored on a cloud-based server or shared drive does not mean there are no confidentiality or security protocols in place." ECF No. 161 at 2. While email is not necessarily a secure method of transmission, it likely is not used to transmit more than a few files at a time, which, in isolation, are unlikely to contain the "crown jewels" of Defendants' confidential information. Second, the Court disagrees

with American Patents’ argument that failure to include this provision would be “fundamentally unfair for Defendants to impose additional burdens that Defendants do not require of themselves or third parties.” ECF No. 160 at 6. If anything, in the Court’s view, American Patents proposes to be treated differently—more favorably—than Defendants treat third-party customers and developers because Defendants will generally require that third-parties access the source code only by using elaborate security protocols (*e.g.*, username and password, two-factor authentication, encryption, VPN, *etc.*), while there is no comparable, on-going security guarantees when source code is produced without the appropriate HIGHLY CONFIDENTIAL – SOURCE CODE designation. Under American Patents’ proposal, there are insufficient guarantees to protect Defendants’ source code “crown jewels.” Third, American Patents’ proposal potentially dramatically increases the burden on Defendants (by requiring them to potentially identify every single file that may have ever been emailed, transmitted over a public network, or stored on the cloud) in order to comply with the protective order and/or is unworkable for the same reason. The Court believes that this burden is far too onerous to be efficient or practical. Fourth, American Patents proposal may actually require yet another round of briefing because it is not precise enough. For example, suppose Defendants emailed a particularly relevant source code file to a third-party. Under American Patents’ proposal, it is unclear whether Defendants must produce just that source code file without the appropriate HIGHLY CONFIDENTIAL – SOURCE CODE designation or if they must produce all versions of the source code file in the same manner. Similarly, it is unclear if Defendants would need to produce any files that were effectively “incorporated by reference,” *e.g.*, `#include`, in the same manner. Likewise, if Defendants emailed that source code file with respect to one accused product, it is unclear whether Defendants would need to produce product-specific variants and/or other versions of that source code file for

other accused products. By comparison, Defendants’ proposal is easy to administer and provides clear boundaries. Fifth, the second part of American Patents’ proposal (“provided to third party developers or similar third parties”) has the potential to swallow the entire rule requiring source code to bear the HIGHLY CONFIDENTIAL – SOURCE CODE designation. More specifically, suppose Defendants provided one build of source code on a DVD to a third-party partner. In that situation, under American Patents’ proposal, it would appear that Defendants would need to produce all of their source code without the HIGHLY CONFIDENTIAL – SOURCE CODE designation. As such, the exception would become the rule and thus undermine the purpose of source code-specific provisions.

For at least these reasons, the Court finds that American Patents’ proposal should not be included in the final protective order.

III. Section 11(a): Exception for storage of Attorneys’ Eyes Only and Source Code inside the United States

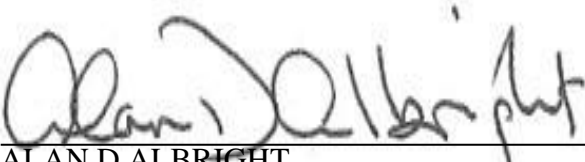
American Patents proposes the following exception for the storage of “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” or “HIGHLY CONFIDENTIAL – SOURCE CODE” within the United States. More specifically, American Patents proposes that the aforementioned designated materials be stored within the United States “provided that Producing Party only stores and allows third parties to store such materials within the United States.” ECF No. 159, Ex. C at 5. After reviewing the Parties’ briefing, the Court finds that American Patents’ proposal should not be included in the final protective order for the reasons that follow. First, the Court agrees with the reasons Defendants recite in their response brief. ECF No. at 4–8. Second, in the Court’s view, excluding American Patents’ proposed provision does not necessarily prohibit American Patents from using iRunway’s litigation-related services. For example, iRunway could set up servers in the United States (which may be a prudent business decision anyways) or iRunway

personnel could access confidential materials on a server located in the United States from Bangalore, India. While that may not be as convenient for iRunway personnel, the Court finds that this inconvenience is more than balanced by limiting the risks of broader dissemination of Defendants' confidential material.

IV. Conclusion

The Court **ORDERS** that the parties submit a final proposed protective order reflecting the Court's guidance contained herein on or by October 11, 2019.

SIGNED this 9th day of October, 2019.



ALAN D ALBRIGHT
UNITED STATES DISTRICT JUDGE